

# **EXHIBIT F**



**Report for**

Houthoff Buruma Coöperatief U.A. in Rotterdam

**Regarding**

Examination of Pictures - H. Mees



## FOREWORD

Dear user of this report,

SBV Forensics B.V. (hereinafter SBV Forensics) is specialised in (internal and external) prevention, examination and/or remedying of irregularities, illegalities and/or punishable acts and therefore aims to establish the truth.

The objective or absolute truth does not de facto exist. However, the examination carried out by SBV Forensics can provide a basis for conclusions that reflect the most probable truth. The highest degree of certainty that can be provided by an expert with respect to facts reconstructed after the event is 'with a probability bordering on certainty', also referred to as 'incontrovertible'. The lower limit lies at 'with a probability bordering on certainty'. And in between there are a number of varying degrees of (im-)probability. On a scale this is reflected as follows:

Probability	Qualification
100 %	With a probability bordering on certainty
90 %	Most likely
75 %	More than likely
50 %	Likely
0 %	Denial of any opinion
-/- 50 %	Unlikely
-/- 75 %	More than unlikely
-/- 90 %	Most unlikely
-/- 100%	With an improbability bordering on certainty

This report is a 'work' within the meaning of article 10 of the Dutch Copyright Act 1912 and is usually provided 'strictly confidential' to the commissioning party. The copyright to this work is vested in SBV Forensics. Dissemination or use hereof without the prior approval of SBV Forensics is, other than in the cases by or pursuant to the law or case law, therefore not permitted (article 31 et seq. Copyright Act 1912). The ban on dissemination and use also applies to the successive acquirers.

SBV Forensics

TABLE OF CONTENTS		Page
<b>2</b>	<b>Assignment .....</b>	<b>1</b>
<b>3</b>	<b>Source data.....</b>	<b>1</b>
3.1	Hard disks.....	1
3.2	Pictures .....	2
3.3	E-mail messages with picture .....	3
3.4	Affidavit and Exhibit 9 .....	3
<b>4</b>	<b>Creation of Pictures .....</b>	<b>3</b>
4.1	Introduction .....	3
4.2	Findings.....	3
4.3	Evaluation.....	10
<b>5</b>	<b>Presence of files on hard disks.....</b>	<b>11</b>
5.1	Introduction .....	11
5.2	Presence of files.....	11
5.3	Deleted files .....	12
5.4	Secure erasure of files .....	13
5.5	Evaluation.....	15
<b>6</b>	<b>Email messages 'me myself and I' .....</b>	<b>16</b>
<b>7</b>	<b>Email messages 'I miss you' .....</b>	<b>16</b>
<b>8</b>	<b>Rule for storing attachments .....</b>	<b>17</b>
8.1	Introduction .....	17
8.2	The way the 'rule' works .....	17
8.3	Ratio for the use of the 'rule' .....	18
8.4	Evaluation.....	19
<b>9</b>	<b>Concluding remarks .....</b>	<b>19</b>

## **1 Introduction**

In proceedings between Mrs H. Mees (hereinafter referred to in short as: the Client) and Mr W.H. Buiter and Mrs A. Sibert Buiter (hereinafter jointly referred to in short as: the counterparty or separately as: Buiter or Sibert) questions arose regarding the creation and origin of approximately 1,250 images on a USB stick sent to us by Houthoff Buruma (hereinafter the Pictures). We were informed that this USB stick is a copy of a USB stick provided by Buiter to the Client's lawyers.

With a view to answering these questions, the Client's Dutch lawyer, professor dr. M.E. Koppenol-Laforce, instructed SBV Forensics on behalf of the Client to examine the properties of these Pictures. Furthermore, with a view to being able to form an opinion with regard to the source of these Pictures, SBV Forensics was also provided with three so-called images of hard disks of (laptop) computers belonging to the Client.

## **2 Assignment**

Having regard to the above, the following assignment was agreed upon:

*"SBV Forensics will examine the properties of the Pictures with a view to establishing the most probable method of creation. SBV Forensics will also examine three images of hard disks of (laptop) computers belonging to the Client with a view to establishing whether the relevant Pictures were created with one of the computers she used, or whether these Pictures were found on one of these computers, and whether these Pictures were sent from one of these computers to Mr Buiter.*

*In addition, SBV Forensics will examine a picture created by the Client as sent by her by email to Mr Buiter, and compare this with the Pictures."*

On performing the activities we discovered another picture<sup>1</sup> created by the Client and sent by her to Mr Buiter. As requested by the Client's Dutch lawyer, we also examined this picture and compared it with the other Pictures.

The Client's Dutch lawyer has informed us that Buiter has declared that he installed a small 'program' which ensured that attachments to email messages were saved separately to a specifically designated location. The Client's Dutch lawyer has instructed us to assess the use of the 'program'.

## **3 Source data**

### **3.1 Hard disks**

SBV received an external hard disk from the Commissioning Party which contained three so-called images.

An image (created in a forensically sound manner) is a bit-by-bit duplicate of a data carrier that, accordingly, is completely identical to the source data carrier. Through the

---

<sup>1</sup> The Dutch version of this report uses the word 'afbeelding', which translates to 'image'. To avoid confusion with the technical term 'image' used to describe a copy of a data carrier, throughout this report, the word picture is used to describe a (digital file containing a) (photo)graphic depiction.

forensically sound creation and processing of an image, digital forensic examination can be carried out without any risk that the digital evidence will be lost or altered.

The images received by us were stated to be created on three (laptop) computers used by the Client. The images received can be described as follows:

*"MacBook"*

Brand hard disk	:	Toshiba MK6034GSX
Serial number	:	Z6EIT1ZJT
Capacity	:	55.8 GB (60.011.642.880 Bytes)
Image created on	:	30-04-2015
SHA hash	:	d95f566eb67b44c60ab6675a7125598f69- aae920a26f70f928410690abd41574

*"MacBook Pro"*

Brand hard disk	:	Fujitsu MHV2120BHPL
Serial number	:	NW81T6825U59
Capacity	:	111.7 GB (120.034.123.776 Bytes)
Image created on	:	27-02-2015
MD5 hash	:	8F4C46823F9B913636B6504C258FD4BE

*"MacBook Primary"*

Brand hard disk	:	Hitachi HTS545025B9SA02
Serial number	:	100726PBL200CSHAH90N
Capacity	:	232.8 GB (250.059.350.016 Bytes)
Image created on	:	27-02-2015
MD5 hash	:	8F248A43122AB50C5AC7EB8C0E0F8BCF

Based on the data found, we consider it most likely that the images have been created in a forensically sound manner. To examine the images we received we processed them with Forensic Tool Kit version 5 of Access Data.

It is clear to us from the examination of the images that there is no partition on any of the above-mentioned computers on which the Windows operating system is or can be installed. Neither do the above-mentioned computers contain virtualization software by means of which the Windows operating system can be used in a 'virtual machine'.

### 3.2 Pictures

For the purpose of our examination we also received a USB stick containing 1,250 Pictures in JPEG format (.jpg), among others. According to the file properties these Pictures were last modified on 15 December 2013.



### **3.3 E-mail messages with picture**

The Client's Dutch lawyer informed us that the Client sent several email messages to Buiter in mid 2011. The subject of these messages was always 'me myself and I'. These messages included an attachment with a file with the name 'moi.jpg.' This relates to a picture that the Client acknowledges to have created herself.

The Client's Dutch lawyer has provided us with these email messages for the purpose of our examination. Our findings in relation to this picture are included in chapter 6.

### **3.4 Affidavit and Exhibit 9**

The Client's Dutch lawyer has informed us that Buiter declared in an Affidavit dated 11 August 2015 that he installed a small program which ensured that attachments to email messages were saved separately to a specifically designated location. An example of such a program was allegedly attached to the Affidavit as Exhibit 9.

The Client's Dutch lawyer has provided us with a copy of the Affidavit and Exhibit 9. Our finding with regard to the use of this 'program', as described in aforementioned documents, are included in chapter 8.

## **4 Creation of Pictures**

### **4.1 Introduction**

As stated in paragraph 3.2 we received the Pictures for analysis. The file names comprise sequential numbers placed between brackets, followed by the extension .jpg.

The file names run from (1).jpg up to and including (1387).jpg. Various intervening numbers are missing. We do not know whether the missing numbers exist or existed.

This chapter contains the findings of our analysis of the Pictures, with a view to being able to determine the most probable method of creation.

### **4.2 Findings**

#### *Numbers of pictures*

As also stated in paragraph 3.2 we received a USB stick containing 1,250 Pictures in JPEG format.

A so-called hash value can be calculated using a complicated algorithm for each digital file. For this purpose various algorithms are used of which the most common are MD5, SHA1 and SHA256.

The chance that different files will have the same hash value is extremely small (whereby it holds that the more complicated the algorithm, the longer the hash value and the smaller the chance). A hash value can therefore be regarded as a digital fingerprint or the digital DNA of a file: the file is identified by the hash value.

In this respect it must be pointed out that it concerns the file content. Two files with different names and different file extensions (for example, Photo1.jpg and Picture2.gif) will have the same hash value if they have the same content. The reason being that the file name is not embedded in the file but is recorded by the file system.

We determined the MD5 hash value for the 1,250 Pictures to be analysed. By comparing these MD5 hash values, we established that 33 photos appeared 2 or 3 times (in total 88 files). Accordingly, we received 1,195 unique pictures.

The USB stick contains not only the Pictures, but also a PDF file called 'Mees Pictures.pdf'. This file comprises 1,388 pages, with one photo on each page.

The type (picture, text etc.) of a specific file can be established on the basis of unique codes at the beginning and at the end of the file.<sup>2</sup> A data carrier can be examined using specific software, such as the investigation software we use, on the basis of the code that alludes to the beginning of a file of a certain type (for example a JPEG file) and to a corresponding code for the end of a file of that type. Both codes and the intervening data will therefore be considered and interpreted as a file of that type. This process is known as 'data carving'. Data carving can, however, also be applied to a file so that embedded elements such as pictures, can be identified.

The investigation software used by us could, through data carving in the 'Mees Pictures.pdf' file, identify 1,282 JPEG pictures. By comparing the MD5 hash values, we determined that these did not contain any duplicates. The 'Mees Pictures.pdf' file therefore contains at least 1,282 unique pictures. (The result of data carving is determined by the condition of the source material on the one hand, and the software used for data carving on the other hand. It is therefore possible that there are more embedded pictures in the file than found by the software. For that reason reference is made to 'at least' the number of files mentioned.)

Four PDF files 'Exhibit L Photographs Mees Sent Buiter [number sequence].pdf' were sent to the Client's lawyer by the counterparty.<sup>3</sup> These four files contain 1,252 pages, with one picture on each page. The first page contains picture that has a strong visual likeness to the picture 'moi.jpg' as sent by The Client to Buiter by email (see also chapter 6). This picture, or at any rate a picture with a strong visual likeness thereto, is not on the USB stick and also does not appear in the earlier 'Mees Pictures.pdf' referred to. The investigation software used by us could, through data carving in this file, identify 1,196 JPEG pictures. By comparing the MD5 hash values, we determined that 9 pictures appeared twice. The four PDF files of Exhibit L accordingly contain at least 1,187 unique pictures.

---

<sup>2</sup> The file name and the extension attached thereto (for example, Textfile.doc) are not part of the file, but are registered by the file system. If the name of the example file is changed to Textfile.jpg, it can still be identified as a file that can be opened by means of a word processor on the basis of these codes.

<sup>3</sup> The Client's Dutch lawyer has informed us that the Exhibit L files ('Exhibit L Photographs Mees Sent Buiter 1-300.pdf', 'Exhibit L Photographs Mees Sent Buiter 301-600.pdf', 'Exhibit L Photographs Mees Sent Buiter 601-900.pdf' and 'Exhibit L Photographs Mees Sent Buiter 901-1252.pdf') were sent by Buiter's American lawyer to the Client's American lawyer on 10 October 2014. The Client received these files from her lawyer on 13 October 2014 by email.

We have summarised the above-mentioned findings in the following table:

	<b>USB stick (1,250 JPEG files)</b>	<b>USB stick (‘Mees Pictures.pdf’)</b>	<b>Exhibit L (PDF files)</b>
Number of files	1,250	1	4
Number of pictures	1,250	1,388	1,252
Identified on the basis of data carving	Not applicable	1,282	1,196
Duplicate pictures on the basis of files	33	Not applicable	Not applicable
Duplicate pictures on the basis of data carving	Not applicable	0	9
Number of unique pictures	1,195	$\geq 1,282$	$\geq 1,187$

**Table 1** – Summary overview numbers of pictures

From the above it follows that it is not clear which files the Client allegedly sent to Buiter by email. In this chapter we restrict ourselves to the 1,250 Pictures (comprising as already stated 1,195 unique pictures).

### *File names*

Devices for recording digital images use a convention for the naming of the resulting files. A digital camera customarily uses the code DSC (an abbreviation for Digital Stills Camera) followed by a sequential number or a combination of date and sequential number.

When using the functions of the operating system of a computer (for example, the function to create a screen image) or specific applications, the software determines which naming convention is used. In addition, the moment when the image is created is usually included in the file name.

Nevertheless, there are also applications that use a naming convention with only a sequential number or a combination of a descriptive element (for example, ‘picture’) followed by a sequential number. Furthermore, there are two variants in practice.

The first variant relates to the application where each time that it is started up and used, again begins with the lowest number. The second variant relates to the application that uses a number that directly follows the highest number found. This second variant is not common in practice and then, in particular, in relation to applications that always save files to a default file location.

As will be set out in more detail below, it can be concluded from the picture content that the Pictures were created in a couple of separate sessions.

Taking into consideration that the file name contains only a sequential number as well as the fact that numbering did not restart at the first Picture from a new session, we deem it most unlikely that the Pictures were initially captured with the file names as used on the USB stick.

This implies that it is most likely that the file names were changed later on into (only) a sequential number placed between brackets. The large number of files makes it most unlikely that the file names were changed manually, accordingly it is most likely that a specific tool or specific functionality of the operating system of the computer was used. Given that an uninterrupted number sequence is used on automated execution of this type of task, we accordingly deem it most likely that also the currently missing numbers were attributed to (picture) files in the aforementioned process.

In combination with the findings from table 1, this justifies the conclusion that the USB stick does not contain all Pictures that exist or existed.

#### *Composition and picture content*

The Pictures were created in a few separate sequences, each sequence comprising various pictures with the same, fixed background: a fixed camera position was used. In addition the position of the Client, as appearing on the Pictures, furthermore shows a relatively minor movement.

Besides, given the position of the Client she was not able to operate the recording device. It is explained below why a function to delay the recording moment ('self-timer') was not used.

The sharpness of the Pictures is, in particular, as a consequence of the image noise, quite low. Nevertheless, it seems as if there was a relatively large depth of field: in other words, that both subjects close to the lens as well as subjects further away from the lens are sharply recorded. This points to the use of a lens with a short focal length. Because the photos show no strong perspective deviation of parts that are close to the camera, it follows from the focal length used that a normal field of view or moderate wide-angle was used.<sup>4</sup> A normal field of view or moderate wide-angle with a short focal length indicates a small image sensor.

The Pictures show a large quantity of "noise". On the one hand this also suggests a small image sensor and on the other hand it indicates little light as is usually the case indoors. It can be concluded from the absence of strong shadows that no additional light sources, such as a flash or a permanent (auxiliary) lamp, were used to compensate for the limited light quantity.

On the basis of the compositions and picture content, we deem it most likely that the images belonging to one series were made briefly after one another. The short time between successive images suggests that no "self timer" was used. Therefore it is most likely that the Pictures were not realized through actions of the Client on or briefly before the moment of the recording.<sup>5</sup> The Pictures were most likely made with the use of a recording device with a lens with a short focal length and a small image sensor, without the use of auxiliary lighting.

---

<sup>4</sup> A normal field of view is understood to mean one that, in terms of perspective, corresponds with that of the human eye. A lens with a wider field of view is referred to as a 'wide-angle lens, a smaller field of view as a 'tele photo lens'. A wide-angle lens relatively enlarges subjects that are close to the lens as a result of which the natural proportions are distorted. For a full screen portrait photo made with a (ultra) wide-angle lens it is characteristic that the nose of the portrayed person is shown as much too big. Conversely, a (long) telephoto lens has a compressive effect.

<sup>5</sup> Below we separately discuss the possibility of recording a video from which stills are separately stored as pictures afterwards.

### *File format and picture size*

The Pictures are all in the file format JPEG. This is a generally customary, compressed file format for pictures (similar to the MP3 format for audio files), in which the compression is applied to reduce the file size at the expense of some image quality.

The files are mainly in the format 640 pixels wide and 480 pixels high. Therefore there is a 4:3 aspect ratio (ratio between width and height). This format is also referred to as 'VGA resolution'. A limited number of images, 69, has a 4:3 aspect ratio, but is smaller in size: 320 x 240 pixels.

Digital single-lens reflex cameras or system cameras, with some exceptions (this particularly concerns the cameras with a so-called Four Thirds or Micro Four Thirds sensor as well as some systems for professional use) have an aspect ratio of 3:2.

The aspect ratio 4:3 is particularly used as (standard) aspect ratio by compact cameras, mobile phones, video cameras that do not support HD format and webcams such as those built-in or connected to computers.

The picture size 640 x 480 pixels, in total therefore over 300,000 pixels, is much more limited than the number of pixels of a photo made with a compact camera: with compact cameras, the picture size is shown in millions of pixels ('megapixels'). The VGA resolution has also for a long time been the standard for the cameras of mobile phones and webcams. Such cameras have a small sensor and use a lens with a short focal length.

The picture size and the aspect ratio of the Pictures (VGA resolution) as well as the picture content (in particular the large quantity of noise and the large depth of field, which are both indicators for a small image sensor) and the fixed camera position are in accordance with the use of a webcam (connected to a computer or built-in to a computer) or a mobile phone (also see below).

### *Meta data*

Meta data is added to digital files on several levels. This occurs for instance on the level of the file system, the part of a computer system that is responsible for the systematic writing, reading and deleting of files: for instance, the file system registers when a file was made, when it was last modified etc.

The so-called EXIF standard has been developed to add meta data to picture files. Devices that support this standard can add meta data to (certain types of) files in which the picture created by the device is recorded.

A compact camera that records a photo as a JPEG file can include EXIF data in that file, such as the focal length of the lens, the diaphragm settings, the used shutter speed etc. What information is added to a picture file as EXIF data is determined by the developer of the recording device.

We established that only very limited EXIF data is present in the provided files. More specifically this concerned: a resolution of '96 dpi', flash mode 'no flash', ISO value '0', exposure mode 'Unknown' and white balance 'Automatic'.

The limited EXIF data is an additional indicator that the Pictures were not made with a digital camera.

Also when using the camera of a mobile phone, more EXIF data is added to the JPEG picture file, such as for instance the make and type of the telephone (for an example also see chapter 6). The absence of these details is a strong indicator that no mobile phone was used to make the pictures.

### *Video*

Before 'HD Ready' and 'Full HD' (an aspect ratio of 16:9 and an image size of 1,280 x 720 pixels, respectively 1.920 x 1.080 pixels) were generally marketed, digital video cameras (or the video functions of compact cameras and mobile phones) used what is retrospectively called 'SD' (standard definition, the image size also known as VGA resolution of 640 x 480 pixels in an aspect ratio of 4:3).

It is therefore conceivable that the Pictures were made through the production of a video file, from which stills were saved as separate Pictures afterwards with software.

EXIF data is also added to video recordings.<sup>6</sup> However, this data is very limited. Various EXIF data found in the Pictures, such as regarding the use of a flash, are usually not recorded in video recordings. Therefore we deem it most unlikely that the Pictures were made by storage from separate images from a video recording.

### *Use of a webcam*

On the basis of the above we deem it most likely that the Pictures were made with the use of a webcam. There are nevertheless various manners in which the picture of a webcam can be recorded into a file.

The first and most obvious method is the use of functions used for that purpose in the software with which the webcam is controlled. There are various applications that use a webcam. This particularly concerns applications that are focused on the realization of a remote picture connection. The best known examples hereof are applications for video phone calls / video chats, such as the platform independent Skype application or the program limited to the Apple platform called Facetime.

Many of such programs offer the possibility to record the picture of the webcam (a video stream) during a session. Initially only as a (still) picture later on also sometimes as a video.

As the counsel of Client, professor dr. Koppenol-Laforce informed us, the Client was regularly in touch with Buiter.<sup>7</sup> A Skype application offers the possibility to record the picture of the webcam of the session partner during a Skype session. This function was initially called 'Video Snapshot', but in later versions of the application it is called 'Take Picture'.

---

<sup>6</sup> The EXIF standard was developed for still images. However, upon opening video files in an image editing program EXIF data is shown.

<sup>7</sup> In our investigation of the images made available to us, we established that Skype was installed onto all three computers of the Client. On all three images (of the hard disks of the computers) we found files in which the history of Skype sessions is recorded through the Skype application.

In the versions of the Skype application developed for the Apple platform, however, the 'Video Snapshot' or 'Take Picture' function is missing. This is because the operating systems for Apple computers, Mac OSX, elaborate functions are already built-in to record pictures. The 'screen shots' recorded by Mac OSX are stored in the PNG format instead of the JPEG format.

Apple computers are always provided with an application with which photos can be taken with the aid of the webcam of the computer. This application does store the images in the JPEG format, but in the process records the name of this application, Photo Booth, as a IPTC field.<sup>8</sup> However, this information is not included in the meta data of the Pictures made available for analysis.

Applications in which webcams are used for the realization of video connections, usually offer the possibility to make two video streams visible on screen: the picture that is recorded through the webcam of the session partner, but also the picture of the own webcam (often shown as 'picture in picture'), so that the computer user can for instance easily check if it is 'fully in screen'. In order to avoid coordination problems with the computer user, the picture of the own webcam is shown in mirror image. If this image is recorded in the form of a screen shot, this therefore results in a mirror image. This is also the case when using the Photo Booth application mentioned above with its standard settings.

Research on the internet pointed out that various versions of Skype for Windows allegedly had the possibility to mirror the image of the webcam horizontally, so that a correct picture can still be presented. We did not find indications that such a setting is also present in Skype versions for Mac OSX, however, we have not carried out elaborate investigations into this matter.

As the Dutch counsel of the Client informed us, the Client in any case had Skype sessions with video connection with Buiter in the period around 2009-2012.<sup>9</sup> In this period various laptop computers of Apple already had a built-in webcam with a resolution of 1,280 x 1,024 pixels. For the control of this webcam, software developers could use the so-called APIs developed by Apple. However, these only supported a 640 x 480 resolution ('high quality video') or 320 x 240 ('standard quality video'). This clarifies why the Skype partners of an Apple user with a high resolution webcam (at that time) still only received pictures in a lower resolution.<sup>10</sup>

### *Picture resolution*

The picture resolution can also be stored in the EXIF data of a picture file. This term is in a way confusing because for the term of the picture size (the total number of pixels that form a picture) the term resolution is also often used.

<sup>8</sup> IPTC is a standard for meta data that can be added to pictures. Where EXIF data is focused on and follows from the (settings on the) device with which the pictures were made, IPTC is mainly focused on the picture content. In this way, keywords can for instance be recorded which provide a description of the content of the picture ('house', 'tree', 'sunset') or the contact details and copyright notice of the photographer. IPTC data must usually be added by the user afterwards. The automatic addition of an IPTC label 'Photo booth' is therefore atypical.

<sup>9</sup> On the images of the computers of the Client, we found various databases in which the Skype application stores the history of Skype sessions. In these databases we established that during various Skype sessions a registration number of a picture recording device was registered. These numbers most likely refer to the built-in webcams of the computers of the Client. Because for our investigation we exclusively had the disposal of the images as mentioned in chapter 3, and not the computers, we have not been able to verify this.

<sup>10</sup> See for instance <https://discussions.apple.com/thread/2293095?tstart=0>.



Picture resolution is the number of pixels that is shown per unit of the output device. The picture resolution is stated in dots per inch (dpi).<sup>11</sup>

While in an Apple environment and also in respect of the majority of the digital cameras a default resolution of 72 dpi is given to pictures,<sup>12</sup> the default resolution that is used by Windows for pictures is 96 dpi.

As indicated above, the resolution of the Pictures is 96 dpi according to the EXIF data. This is a strong indicator that the Pictures were recorded within a Windows environment.

#### *Adjustment of files*

It cannot be ruled out that the Pictures were initially created in another picture form (moving images instead of stills) with another picture size and/or another file format and were changed afterwards. Editing picture form, picture size, picture resolution and file format is after all possible with nearly every video application and/or image editing application. It is also very easy to edit file properties and/or EXIF data with various simple tools which can for instance be found on the internet.

If the Pictures were manipulated with the aid of the applications on the computers of the Client, the end result (the 1,250 Pictures, either or not in an edited form) should at some time also have been stored on the computers of the Client. However, as will be set out in greater detail in chapter 5, we have not found indicators of this.

### **4.3 Evaluation**

Given, inter alia, the file size, the camera position, the depth of field and the meta data, we consider it most likely that the Pictures that were submitted for analysis were originally created using a webcam. Furthermore, given the picture resolution we consider it most likely that the initial storage of these pictures took place in a Windows environment.

As pointed out in chapter 3, we did not find a Windows environment or virtualization software on the images. Therefore, we consider it most unlikely that the Pictures were initially stored on one of the Apple computers used by the Client.

---

<sup>11</sup> Use of this standard unit is not undisputed or at least not always equally accurate. Dependent of the type of output device (old TV screen, modern LCD screen, ink jet printer, raster image processor etc.) sometimes the term ppi (pixels per inch) or lpi (lines per inch) more suitable. In practice usually dpi is simply referred to.

<sup>12</sup> Apple's own application Photo Booth is a remarkable deviation: dependent of the version and the computer on which it has been installed, the picture resolution is sometimes registered and sometimes not registered in the EXIF data. On a modern iMac operating with Mac OS 10.10, Photo Booth registers a picture resolution of 72 dpi in the EXIF data. The picture discussed in chapter 7 which was found on the image of the 'Macbook Pro' does not contain any picture resolution in the EXIF data.

## **5 Presence of files on hard disks**

### **5.1 Introduction**

We pointed out in chapter 4 of this report that the Pictures were most likely originally created by using a webcam and were initially stored in a Windows environment.

Even though we consider this most unlikely, it cannot be fully excluded that the Pictures were created with a recording device linked to a computer of the Client, whether or not operated by a third party.

For example, in theory, it is possible that a screen shot was made of the mirrored webcam picture and the specific picture was subsequently edited in an image editing program and flipped horizontally in doing so, after which the EXIF data of the file were adjusted, by means of a specialised tool, to the values we found in the files. However, performing this picture editing manually is very time consuming.<sup>13</sup>

Likewise, it is possible in theory that a video file was created, of which individual pictures were saved as separate files, after which the EXIF data were also adjusted by means of a specialised tool. However, the process of manually creating a still picture from a video file is very time consuming.<sup>14</sup>

Furthermore, the Dutch lawyer of the Client informed us that the other party asserts that the Client sent the Pictures by email.

In order to examine whether these options may have occurred, we examined the images of the hard disks from the computers of the Client for relevant digital evidence.

### **5.2 Presence of files**

The three images contain a total of 871,147 graphic files. In total, 430.615 of these files are in JPEG format.

It is infeasible in the course of a brief examination to assess the contents (in other words: visually) of such a large number of files. For this reason, we therefore used a different method to establish whether the files containing the Pictures are on the images.

As is also explained in paragraph 4.2, a so-called hash value can be calculated using a complicated algorithm for each digital file. For this purpose various algorithms are used of which the most common ones are MD5, SHA1 and SHA256.

---

<sup>13</sup> Manually editing the Pictures in the manner stated above requires the pictures to be opened, edited and saved again in several applications (both an image editing program and an EXIF tool). Therefore, this is a very time-consuming process. Several applications for editing pictures have the option to process multiple pictures at the same time (batch processing) or to apply multiple successive edits on multiple files (such as performing 'actions' in Photoshop). The use of batch processing or similar techniques requires more than average knowledge of the specific software. Furthermore, it must be considered that the files are stored in the JPEG format. As indicated earlier, this is a compressed format. If these files are edited and saved again, the file compression will cause the picture quality to deteriorate more and more. Whether the picture quality deteriorates as a result of repeated compression is difficult to establish and we have not examined it either.

<sup>14</sup> Because the moment on which the still picture is extracted must be selected by the user, this step will most likely always be performed manually. For the subsequent editing of these pictures, the same findings apply as indicated in the previous footnote.

The chance that different files will have the same hash value is extremely small (whereby it holds that the more complicated the algorithm, the longer the hash value and the smaller the chance). A hash value can therefore be regarded as a digital fingerprint or the digital DNA of a file: the file is identified by the hash value.

In this respect it must be pointed out that it concerns the file content. Two files with different names and different file extensions (for example, Photo1.jpg and Picture2.gif) will have the same hash value if they have the same content. The reason being that the file name is not embedded in the file but is recorded by the file system.

We determined the MD5 hash values for the 1,250 Pictures to be analysed. Subsequently, we also calculated the MD5 hash values for all 871,147 graphic files on the images.

If the aforementioned 871,147 graphic files also contain one or more of the 1,250 Pictures, whether or not with a modified file name, then the MD5 hash values must be identical. However, we established that there are no identical hash values. Therefore, it can be concluded with a probability bordering on certainty that none of the 1,250 Pictures were found on the images of the Client's computers.

### **5.3 Deleted files**

If a file is deleted by a user, it is not physically deleted from the data carrier. Only the reference to the location on which the file is saved on the data carrier is removed by the file system. The relevant storage space on the data carrier is released by the file system, so that other files can be saved on that same location. In due course of time, a file that has been "removed" by a user will be physically overwritten.

By physically reading out a data carrier bit by bit, removed files can be recovered at a later time, at least as long as they have not been overwritten by other files.

With the help of the FTK program we used for this investigation, we also examined the images for deleted files. Simply put, in doing so, the software searches for the code that alludes to the beginning of a file of a certain type (for example, a JPEG file) and to the corresponding code for the end of a file of that type. Both codes and the intervening data will therefore be considered and interpreted as a file of that type. This process is known as 'data carving'.

The files recovered as a result of data carving were also included in the analysis of MD5 hash values that was described in the previous paragraph. Therefore, it can be concluded with a probability bordering on certainty that none of the 1,250 Pictures have been stored on the Client's computer, were later deleted and could still be fully recovered.

However, if the intermediate data has been partially overwritten, or corrupted, the file content will no longer be identical to that of the original file. In that case, comparing the MD5 hash value cannot give a definite answer on whether one or more of the 1,250 Pictures have been stored on the Client's computer, were later deleted but could not be fully recovered.

Only a visual assessment can give a definite answer in this respect. In the free disk space (i.e., the disk space that, according to the file system, is available to store new files) a large number of JPEG files which have been fully or partially recovered through

data carving are located on the images, which files we have visually assessed for similarities with the 1,250 Pictures.

On the hard disk of the MacBook, this is a total of 22,808 JPEG files. These files do not contain any files that show a visual resemblance to one or more of the 1,250 Pictures.

On the MacBook Pro and the MacBook Primary, there are 23,981 and 171,923, respectively, fully or partially recovered JPEG files in the free disk space. These files include a large number of files that show a visual resemblance to one or more of the 1,250 Pictures.

Further analysis of the images showed that these Pictures were included in deleted PDF files, which could still be fully recovered through data carving. By comparing the MD5 hash values of these deleted PDF files with the MD5 hash values of PDF files that had not been deleted yet, we could establish that these concerned deleted copies of the files "Exhibit L Photographs Mees Sent Buiter [number sequence].pdf" (i.e. the PDF files the Client received from her lawyer).

That these files were not found when comparing the MD5 hash values as described in the preceding paragraph is not the result of the partial overwriting or corruption of these files.

On the one hand, the differences between the MD5 hash values are the result of the fact that when compiling the PDF files, only the content of the pictures has been enclosed for Exhibit L (in other words: the EXIF data is lacking in these pictures) and on the other hand, the fact that the Pictures were included in the PDF in a smaller format: the majority of the Pictures was reduced in size from 640 x 480 pixels to (for example) 160 x 120 pixels.

#### **5.4 Secure erasure of files**

Files that have been deleted by a user, as explained above, can be recovered as long as the relevant disk space is not overwritten by other files.

However, users can also "securely erase" files. This means that the disk space used by the file that is to be deleted is immediately overwritten with meaningless information.

For this purpose, special tools can be used that overwrite files and/or folders or the entire disk space that is considered freely available by the file system in its entirety with meaningless information.<sup>15</sup>

The operating system for Apple, Mac OS X, was standard already provided with two different options to securely erase files: the Finder, the program to manage and navigate through files and folders, similar to the Windows Explorer program in Windows operating systems, contained the option to securely empty the "Trash". If this option was chosen, the disk space of the files the user transferred to the "Trash" was immediately overwritten with meaningless information.

A second option was included in the tool "Disk Utility" which provided the option to overwrite the full free disk space with meaningless information.

---

<sup>15</sup> Depending on the tool, the disk space is overwritten one or several times with 0 or 1 on bit level or a random pattern thereof. With various tools, the user can choose the manner in which the overwriting takes place.

The use of a tool to overwrite the full free disk space can be noticed in a relatively simple manner in the examination of a data carrier. If in an intensively used computer most of the free disk space merely consists of the value 0 or 1 or a repeating pattern thereof and hardly any deleted files can be recovered through data carving, it is more than likely that such a tool has been used.

Given the large number of files found on the images, the computers of the Client were most likely used intensively. Given the large number of files that could be "recovered" through data carving, we consider it most unlikely that a general tool to overwrite free disk space has been used on these computers.

It does remain theoretically possible that individual files have been removed securely in a way that can be demonstrated hardly or not at all: if individual files are securely erased, as is the case when securely emptying the 'Trash', only small amounts of disk space are overwritten. The use of such a method can be demonstrated hardly or not at all by examining the free disk space. Therefore, it remains theoretically possible that one or more of the 1,250 Pictures (in original size) were ever stored on the hard disks of the Client's computers, but that the Client deleted these Pictures in a secure and irrecoverable manner.

This comes with two comments that most likely preclude the application of such a process by the Client.

In the first place, it must be pointed out that secure erasure in the manners described above does not guarantee that the information cannot be recovered. After all, the recent versions of Mac OS X (from Mac OS X 10.6) provide the option for programs to save files automatically. This way, users can never lose any information because they forget to save their work. In order to make this possible, copies of files are stored by the operating system. However, these copies are not always stored on the same disk location. If a user transfers a file to the 'Trash' and then empties it securely, this specific file has been securely erased. However, any copies of the file made before that time have therefore not been securely erased and can still be 'recovered'. In order to not provide users with a false feeling of security, Apple has removed both options with the introduction of the newest version of its operating system, El Capitan (Mac OS X 10.11).<sup>16</sup>

Even more important is a second observation relating to the operation of the email program 'Mail' on an Apple computer. In order to prevent loss of data or disruption of the due operation of programmes, various folders with files are by default not accessible for users.

On an Apple computer, an individual email message - otherwise than with for example Microsoft Exchange and Microsoft Outlook<sup>17</sup> - is an individual file with an .emlx file

---

<sup>16</sup> The possibility still exists within the operating system, but is no longer offered in the graphical user interface. In order to still apply the functionality, the user must open a session in the program Terminal after which a Unix command can be executed. For example, in order to completely overwrite the free disk space 7 times, the command is 'diskutil secureErase freespace 2 /Volumes/drivename'.

<sup>17</sup> Microsoft Exchange is the mail server application of Microsoft which is responsible for the email traffic within a network. This application stores all email messages of all users of the mail server in a central database (these files have an .edb extension). Microsoft Outlook is a mail client. A user can, among other things, subsequently make a connection with his/her 'mailbox' on the mail server. For offline use, the user can synchronise his/her 'mailbox'. The mail messages are then copied to one locally stored file (with an .ost extension). A user can also choose to archive email messages locally. This also takes place in one locally stored file (with a .pst extension).



extension. These files are stored in a file location with, for example, the following path for sent messages:<sup>18</sup>

`/Users/username/Library/Mail/V2/POP-useraccount/Sent messages.mbox/@@@/0/1/1/Data/Messages/`

In the more recent versions of Mac OS X, the Library folder is no longer shown. The user can only view this folder by holding a special key while clicking the parent folder. The operating system also shows to contain files with an .mbox extension. These are in fact also folders, the contents of which only become visible by holding a special key while clicking the folder. If the user nevertheless manages to gain access to the lowest level, where the individual messages are shown as .emlx files, then it is still not easy to find the file that the user wishes to delete: the files have numbers as file names. The messages must be opened in order to see the specific message. Once the message has been found, it can be subsequently moved to the 'Trash' in order to securely erase it in the abovedescribed method. In order to securely erase individual email messages, specialized knowledge of the Mac OS X operating system is required which a regular user does not have.<sup>19</sup> Furthermore, there exists the risk that the individual deletion - outside of the Mail program - disrupts the operation of the mail program as a result of which the mail boxes must be rebuilt.

An alternative approach is that messages are first deleted in the Mail program and that subsequently, with the help of a tool, the free disk space is completely overwritten with meaningless information. However, we have found no indications for the use of such tools in the above.

## 5.5 Evaluation

The pictures found after data carving - which visually resemble one or more of the 1,250 Pictures (in original size) - concern embedded pictures reduced in size, without EXIF data, which were stored on the Client's hard disks by receipt per email of four PDF files, contained in Exhibit L.

As indicated above, we have found none of the 1,250 Pictures (in original size) among the images stored on the hard disks of the Client's computers.

We deem it most unlikely that one or more of the 1,250 Pictures (in original size) have been stored on the hard disks of the Client's computers but have been deleted in a secure, irrecoverable manner. After all, no indicators were found for the complete overwriting of the free disk space. The secure erasure of individual email messages and related attachments requires highly specific IT knowledge, and what's more, with the most recent versions of Mac OS X (as in any case used on the 'MacBook Primary') the secure erasure of files offers no security that all existing copies of the specific files are erased.

Since none of the original 1,250 Pictures were stored on the hard disks of the Client's computers, we deem it most unlikely that the files were sent per email from the Client's computers to the counterparty, or at least to Buiter. All the more because the secure and irrecoverable erasure of specific email messages requires many actions and

<sup>18</sup> Here, @@@ stands for a randomly comprised folder name, consisting of hexadecimal characters,

<sup>19</sup> As an alternative method, a user can open a session in the program Terminal. Then the user can navigate through the folder structure directly, by using Unix commands. The folder structure is directly visible then. The use of the Terminal possibly requires even more extensive IT knowledge.



very specific IT knowledge and furthermore no indicators were found for the overwriting of free disk space.

## **6 Email messages 'me myself and I'**

As already indicated in paragraph 3.3, the Client's Dutch lawyer informed us that the Client sent several email messages to Buiter in mid 2011. The subject of these messages was always 'me myself and I'. These messages included an attachment with a file named 'moi.jpg.' This relates to a picture that the Client acknowledges to have created herself.

After inspection of the 'moi.jpg' file it appeared to include various EXIF-data. It concerns among other things the recording date ('7-6-2011'), the camera manufacturer ('Research in Motion', the manufacturer of Blackberry smartphones), the camera model ('Blackberry 9300'), the flash mode ('No flash'), and the picture resolution ('72 dpi'). The picture size is 804 x 1,072 pixels.

We have found no file titled 'moi.jpg' on the images of the hard disks of the Client's computers, nor did we find any email messages with the subject 'me, myself and I'.

In combination with the EXIF data presented above, we therefore deem it most likely that the specific photo was made with a Blackberry smartphone. It is possible that this picture was sent using a Blackberry smartphone.

Perhaps superfluously, we would like to remark that we deem it most unlikely, based on the file properties described above in chapter 4 of this report, that the 1,250 Pictures were captured with a Blackberry smartphone.

## **7 Email messages 'I miss you'**

On 31 July, 3 and 4 August 2010, Client sent a total of four email messages to Buiter with either 'I miss you' or the Dutch '*Ik mis je*' as subject. A picture, by the title 'plaatje.jpg', was attached to these messages.

We found the original picture on the image of the 'MacBook Pro', in the 'Photo Booth' folder. This folder is used by the Photo Booth-application as default storage location and is created upon the first use of this application in the user's 'Pictures' folder.

In the EXIF data of this picture, we only found the picture size (640 x 480 pixels). Insofar as we have been able to verify, the Photo Booth application has no options to set the picture size of the images. We furthermore established that the picture resolution is not stored in the EXIF data. As IPTC label is stated the name of the application with which the picture is created ('Photo Booth').

Perhaps superfluously, we would like to point out that it is most unlikely that the Pictures, just like the picture attached to the above-discussed email messages, were created with the use of Photo Booth, for the reason that among the Pictures there are also photos with a deviating, smaller picture size than the default picture size of Photo Booth, but also because the picture resolution of the version of Photo Booth used by Client, or at least the version on the 'MacBook Pro' does not store the picture resolution in the EXIF data, and finally considering the absence of the other EXIF data, such as the flash mode, and the presence of the IPTC label 'Photo Booth'.

## **8 Rule for storing attachments**

### **8.1 Introduction**

The Client's Dutch lawyer has informed us that Buiter declared in an Affidavit dated 11 August 2015 that he installed a small program which ensured that attachments to email messages were saved separately to a specifically designated location. An example of such a program was allegedly attached to the Affidavit as Exhibit 9.

The Client's Dutch lawyer has provided us with a copy of the Affidavit and Exhibit 9, in order to assess the use of this 'program'.

### **8.2 The way the 'rule' works**

Exhibit 9 contains a print of a message on an internetblog, 'Pixelchef.net'. From this it can be deduced that the terminology used by Buiter in the Affidavit is incorrect, or at least inaccurate: there is no 'program' that can be 'installed'.

Email programmes such as Microsoft Outlook, as apparently used by Buiter, usually have the option to automate simple, common tasks. This is done in Outlook by setting a so-called 'rule'. With the help of such a rule a user can, for example, relocate all messages received from a specific email address to a specific folder.

Visual Basic for Applications (VBA) is a feature developed by Microsoft with which 'scripts' (a set of instructions) can be written which can change or expand the functionality and/or operation of applications that support VBA, such as Microsoft Outlook.

In Exhibit 9 is explained how a user can set a 'rule' in Outlook, which runs a VBA script upon receipt of an email message. The VBA script shown in Exhibit 9 stores the attachment to an email message in a folder designated for that purpose in the script.

The original email with the attachment is not replaced or removed as a consequence of the 'rule'. Use of this 'rule' and the application of the script ran by that rule, does also not lead to any changes in the file name.

If several attachments are received with the same file name, the script will overwrite the older file with the same name. For users who do not wish this, the writer of the blog offers the following option as a solution: change some lines in the script to store the attachments with the storage date and time added to the file name.

One cannot deduct from the Affidavit whether Buiter chose this option or went with the standard script.

The counterparty argues that the Pictures were sent by Client to Buiter per email. If this were the case, it is theoretically possible that some photos were sent several times by Client per email. Based on general user habits on the one hand and the fact that the email messages discussed in chapters 6 and 7 were sent several times and were each time accompanied by an attachment with the same file name, we deem it most unlikely that Client used different file names each time she sent one of the Pictures.

This implies that the same file must have been stored several times by the 'rule', in the location as indicated by Buiter in the script ran by that 'rule'. If the standard script of

Exhibit 9 had been used there would have been no double Pictures, since this would have resulted in the overwriting of earlier files with the same file name. In that case Buiter must have used a modified script. If he would have chosen for the solution mentioned in Exhibit 9, the file names of the Pictures should include the storage date and time. However, this is not the case for the 1,250 Pictures on the USB stick.

In this context it is furthermore important to remark that the images discussed in chapters 6 and 7 were sent by email to Buiter several times. Therefore, if the 'rule' was used, these images should be stored on Buiter's hard disk.

The picture in the 'moi.jpg' file is not part of the Pictures on the USB stick, and an image that bears a strong resemblance to the image in the 'moi.jpg' file only appears once in the PDF files of Exhibit L. The image in the 'plaatje.jpg' file is not part of the Pictures on the USB stick and there are no images among the PDF files of Exhibit L that show a strong visual resemblance to the image in the 'plaatje.jpg' file. These findings are not in accordance with the way the 'rule' works.

### **8.3 Ratio for the use of the 'rule'**

In paragraph 11 of the Affidavit, Buiter states that he regularly receives email messages with large attachments which he subsequently has to store. He says that he used the 'rule', or something similar, in order to prevent that, briefly put, the - at the outset - limited storage capacity of the Outlook mailbox would be overwritten as a result of storing these attachments in Outlook.<sup>20</sup>

As a solution for this problem, the option for a 'rule' as described in Exhibit 9 is remarkable, in the sense that the original email with the attachment is not removed from the Outlook mailbox by means of the 'rule'. The risk of exceeding the storage capacity thus remains, unless the user decides to manually remove these email messages from the mailbox. That is why the 'rule' only results in a very limited time advantage but with a serious disadvantage: what remains is a folder with files in respect of which it is no longer possible to establish how these were received, who sent them and which remarks accompanied these files.

There are easier and more effective solutions for the problem signalled by Buiter: a user can set a 'rule' in Outlook with which every email message containing an attachment is moved to a local archive (a locally stored file with a .pst extension). The advantages of this procedure are that the size of the mailbox is reduced directly, the context of the attachment is retained, and that one can still use the search options of Outlook. Such a 'rule' is furthermore much easier to realize, because it can be set with the support of a 'Wizard' in Outlook and no complicated VBA script has to be written and addressed.

---

<sup>20</sup> Up to and including Outlook 2002, the maximum size of the file in which all mail items, contacts, etc. are stored (the Outlook.pst file) is almost 2 GB. The standard limit for Outlook 2003 and 2007 is 20 GB, and for newer versions the limit is 50 GB. Incidentally, these standard limits can be increased for the versions Outlook 2003 and onwards. What's more, storage capacity can easily be increased by creating locally stored archive files.



#### **8.4 Evaluation**

The rule described in Exhibit 9 is an unnecessarily complicated and not very effective solution for the problem identified by Buiter of the (initially) limited mail box capacity in Outlook.

The fact that on the one hand certain of the Pictures are stored twice and on the other hand various versions of "moi.jpg" are missing and the image "plaatje.jpg" is missing altogether, is not consistent with the way the specific "rule" works.

#### **9 Concluding remarks**

We received 1,250 files on a USB stick. The file names of the Pictures run from (1).jpg up to and including (1387).jpg. Various intervening numbers are missing.

Given the customary naming conventions, we consider it more than likely that, after the initial storage of the Pictures, the file names were modified afterwards.

Given the Client's position in the images, she was not able to operate the recording device. Based on the compositions and content of the images it is most likely that the photographs belonging to the same series were made one shortly after the other. This indicates that no "self-timer" was used. It is most likely that the Pictures are not the result of acts carried out by the Client.

The picture size, the aspect ratio and content of the Pictures are consistent with the use of a webcam or a mobile telephone. However, the files contain little EXIF data. That is a strong indicator that the Pictures were not recorded using a digital camera or mobile telephone.

It is most unlikely that the Pictures are the result of storing separate images from a video file.

It is most likely that the Pictures were created using a webcam in a Windows environment. This is indicated by the fact that the Pictures according to the EXIF data have an image resolution of 96 dpi. It is most unlikely that the Pictures were stored on an Apple computer as used by the Client.

It cannot be excluded that the form, size and resolution of the file or the file format have been modified after the original creation. However, in that case the Pictures would have to have been stored on the Client's hard disks at a certain moment. No indicators were found for that.

Based on the hash values of all Pictures on the images, it can be concluded that none of the 1,250 Pictures were found on the images of the Client's computers. The images were also examined for deleted files. Based on the hash values it can be concluded that none of the 1,250 Pictures have been stored on the Client's computer, but were later deleted and could still be fully recovered.

On the "Macbook Pro" and the "Macbook Primary" various images were found that show a strong visual resemblance to one or more of the 1,250 Pictures. This concerned removed copies of the files "Exhibit L Photographs Mees Sent Buiter [number].pdf:.". The images contained therein could not be found based on the hash values, because these images were recorded without EXIF data and in a smaller format in the PDF files.



Given the fact that the computers most likely were used intensively and given the large number of files that could be recovered, it is most likely that no tool was applied to the computers to overwrite free disk space.

The picture "moi.jpg" was most likely made using a Blackberry smartphone. This opinion is based on the EXIF data of the picture, which contain the camera manufacturer and the camera model. It is possible that this picture was also sent using a Blackberry smartphone. E-mail messages with this picture as an attachment were in any case not found on the Client's computers.

The picture "plaatje.jpg" which the Client sent to Buiter several times by email was most probably created using the application Photo Booth on the "Macbook Pro". Given the differences in file properties, it is most unlikely that the 1,250 Pictures were recorded the same way as the picture "moi.jpg" or the picture "plaatje.jpg".

In summary, the observations and conclusions set out above lead to the following final conclusion:

- It is most unlikely that the 1,250 Pictures were recorded by the Client herself. Due to the quick succession of the photographs it is most unlikely that a self-timer was used.
- It is most unlikely that one or more of the 1,250 Pictures (in original size) have been stored on the hard disks of the Client's computers but have been deleted in a secure, irrecoverable manner.
- No indicators were found for the complete overwriting of the free disk space. The safe removal of individual email messages and related attachments requires highly specific IT knowledge.
- It is most unlikely that the Pictures were sent by email to the opposing party or at least to Buiter using one of the Client's examined computers.

We trust to have been of sufficient service to you by issuing this report.

**SBV Forensics B.V.**

On whose behalf

A handwritten signature in black ink, appearing to read "M.G.J. de Gunst".

M.G.J. de Gunst MSc LLM